

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of)
 (Briefly describe the property to be searched)
 or identify the person by name and address))

Case No. 2:18-MJ-01974

342 E. Plymouth Street, Long Beach, California 90805)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California
 (identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B

Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office
 (United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued:

July 31, 2018 2:25 pm



Judge's signature

City and state:

Los Angeles, CA

Hon. Frederick F. Mumm, U.S. Magistrate Judge

Printed name and title

AUSA: J. Mitchell x0698

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 18-MJ-1974	Date and time warrant executed: 8/2/18 6:15 AM	Copy of warrant and inventory left with: Ernesto Hernandez
--------------------------------	--	--

Inventory made in the presence of:

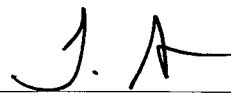
Ernesto Hernandez

Inventory of the property taken and name of any person(s) seized:

- 1) Samsung Galaxy S6 Edge (R58657WTAQT)
- 2) Apple laptop (C02T8MRAH320)
- 3) Chrome thumb drive "COS"
- 4) Alcatel one touch tablet
- 5) ASUS tablet
- 6) Dell computer tower (7KMVLN1)
- 7) Red Apple iPod
- 8) Black Apple iPod

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: **11/1/18**

Executing officer's signature

Timothy A. Special Agent

Printed name and title

AFFIDAVIT

I, Timothy Alon, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so employed since 1995. My responsibilities with the FBI include investigations into the sexual exploitation of children and child pornography in the Central District of California. The FBI is responsible for enforcing federal criminal statutes involving the sexual exploitation of children under 18 U.S.C. § 2251, et seq. During my tenure with the FBI, I have conducted and participated in numerous investigations of criminal activity, including at least 300 investigations in which targets have exploited children using the Internet, typically by transmitting child pornography using computers connected to the Internet. During my investigations in these cases, I have participated in the execution of at least 300 search warrants in which evidence of these violations was seized. I am currently assigned to the Child Exploitation Investigations Group ("CEIG"), which is a task force specifically dedicated to investigating and combating child exploitation. The CEIG task force is operated by the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations.

2. Through my training and experience, I have become familiar with the methods of operation used by people who are involved with offenses involving the sexual exploitation of children. I have attended training classes and seminars concerning computer crimes and the sexual exploitation of children on the Internet. This training has given me an understanding of how people involved with offenses relating to the sexual exploitation of children use the Internet to further those offenses. My experience in investigations in this regard has supplemented my

understanding of how people involved in offenses relating to the sexual exploitation of children use the Internet to further those offenses.

II. PURPOSE OF AFFIDAVIT

3. This affidavit is made in support of an application for a warrant to search the premises located at 342 E. Plymouth Street, Long Beach, California 90805 (the "SUBJECT PREMISES"), more fully described below and in Attachment A, which is attached hereto and incorporated herein by reference, and to seize evidence, fruits, and instrumentalities, as specified in Attachment B, which is also attached hereto and incorporated by reference, of violations of 18 U.S.C. §§ 2252A(a)(2) (receipt and distribution of child pornography), and 2252A(a)(5)(B) (possession of child pornography) (the "Subject Offenses").

4. The statements in this affidavit are based upon my personal observations, my training and experience, my investigation of this case, and, where noted, information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of, or investigation into, this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. PREMISES TO BE SEARCHED

5. The SUBJECT PREMISES is located on a single lot shared with another single-family residence identified as 340 E. Plymouth Street. The 340 E. Plymouth Street residence is the building located adjacent to E. Plymouth Street and has the number "340" at the front of the residence. The SUBJECT PREMISES is located behind the 340 E. Plymouth Street residence. A shared brick styled driveway on the east side of the property leads to the SUBJECT

PREMISES at the rear of the property. On the driveway near the sidewalk are two mailboxes. They are labeled "340" and "342."

6. The SUBJECT PREMISES's exterior walls are dark green in color. A black security door is at the front of the residence. Leading to the front door are two steps. Large windows with white window frames are located on both sides of the front door. Sliding doors are located on the west side of the property. The roof appears to be composed of multi-colored shingles.

IV. ITEMS TO BE SEIZED

7. The items to be seized from the SUBJECT PREMISES are set forth in Attachment B, which is incorporated by reference.

V. SUMMARY OF INVESTIGATION

8. On or about December 8, 2017, SA Joseph Cecchini, an FBI agent assigned to the FBI office located in Tulsa, Oklahoma, used a peer-to-peer program in an undercover capacity to download child pornography. This child pornography was publicly available for download to any Internet user with compatible peer-to-peer file-sharing software, which is available for free over the Internet. The IP address of the computer offering the child pornography relates back to the SUBJECT PREMISES. Thus, there is probable cause to believe that the SUBJECT PREMISES contains evidence of criminal activity in violation of 18 U.S.C. §§ 2252A(a)(2) (receipt and distribution of child pornography), and 2252A(a)(5)(B) (possession of child pornography).

**VI. BACKGROUND REGARDING CHILD EXPLOITATION OFFENSES,
COMPUTERS, AND THE WORLDWIDE INTERNET COMPUTER
COMMUNICATION NETWORK**

9. In this affidavit, the terms “minor,” “sexually explicit conduct,” “visual depiction,” “producing,” and “child pornography” are defined as set forth in 18 U.S.C. § 2256. The term “computer” is defined as set forth in 18 U.S.C. § 1030(e)(1).

10. Based upon my training and experience in the investigation of child pornography, and information related to me by other law enforcement officers involved in the investigation of child pornography, I know the following information about the use of computers with child pornography:

a. Computers and Child Pornography. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. Child pornographers can now produce both still and moving images directly from a common video camera and can convert these images into computer-readable formats. The use of digital technology has enabled child pornographers to electronically receive, distribute, and possess large numbers of child exploitation images and videos with other Internet users worldwide.

b. Storage. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution. Images can also be stored on portable thumb drives and removable, external hard drives.

c. Internet. The term “Internet” is defined as the worldwide network of computers -- a noncommercial, self-governing network devoted mostly to communication and research with roughly 500 million users worldwide. The Internet is not an online service and has

no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an individual computer user must use an access provider, such as a university, employer, or commercial Internet Service Provider (“ISP”), which operates a host computer with direct access to the Internet.

d. Internet Service Providers. Individuals and businesses obtain access to the Internet through ISPs. ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs’ servers; remotely store electronic files on their customer’s behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. Those records often include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data and written record format.

e. IP Addresses. An Internet Protocol address (“IP Address”) is a unique numeric address used to connect to the Internet. An IPv4 IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). In simple terms, one computer in a home may connect directly to the Internet with an IP Address assigned by an ISP. What is now more typical is that one home may connect to the Internet using multiple digital devices simultaneously, including laptops, tablets, smart phones, smart televisions, and gaming systems, by way of example. Because the home subscriber typically only has one Internet connection and is only assigned one IP Address at a time by their ISP, multiple devices in a home are connected to the Internet via a router or hub. Internet activity from every device

attached to the router or hub is utilizing the same external IP Address assigned by the ISP. The router or hub “routes” Internet traffic so that it reaches the proper device. Most ISPs control a range of IP Addresses. The IP Address for a user may be relatively static, meaning it is assigned to the same subscriber for long periods of time, or dynamic, meaning that the IP Address is only assigned for the duration of that online session. Most ISPs maintain records of which subscriber was assigned which IP Address during an online session.

f. IP Address – IPv6. Due to the limited number of available IPv4 IP addresses, a new protocol was established using the hexadecimal system to increase the number of unique IP addresses. An IPv6 consists of eight sets of combination of four numbers 0-9 and/or letters A through F. An example of an IPv6 IP address is 2001:0db8:0000:0000:0000:ff00:0042:8329.

g. Peer-to-Peer. The term “peer-to-peer” (“P2P”) has come to describe applications or programs that allow users to exchange files with each other directly or through a mediating server, via the Internet.¹ A decentralized peer-to-peer file transfer network does not follow a model using different clients or servers; but, rather, it is a network of equal peer computers that simultaneously function as both “clients” and “servers” to the other users on the same network.

h. Open Source. The term “open source” is defined as software that includes a free license; in other words, it is freely available to everyone using the Internet.

i. Share Folder. The term “share folder,” in the context of P2P software, is a folder or directory on a computer’s hard drive, which a P2P user can set up to share his/her

¹ A computer that is performing tasks for other computers that are connected to it is often called a “server.” A “client” computer is one that is connected to a server and is making requests of the server.

contents with other computers on a peer-to-peer network. Most P2P software defaults to allow other users with compatible software on the same peer-to-peer network to browse this share folder, and download files. The term “browsing,” as used in reference to peer-to-peer networks, refers to the ability of a P2P user to look at or browse the shared files of another P2P user.

j. The terms “jpeg,” “jpg,” “gif,” “bmp,” and “art” are defined as graphic image files, namely, pictures.

k. The terms “mpeg,” “mpg,” “mov,” “avi,” “rm,” and “wmv” are defined as video or movie files. To use these video files, one needs a personal computer or other digital devices with sufficient processor speed, internal memory, and hard disk space to handle and play typically large video files. One also needs a video file viewer or client software that plays video files. One can download shareware or commercial video players from numerous sites on the Internet.

11. A growing phenomenon on the Internet is P2P file sharing. P2P file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user’s computer, and conducting a search for files currently being shared on the network. BitTorrent, one type of P2P software, sets up its searches by keywords typically on websites, known as Torrent websites, which are dedicated to servicing the BitTorrent software. Users enter keyword searches into the Torrent website to

identify and locate files of interest. Torrent websites do not contain the actual files of interest.

Rather, the Torrent websites provide a file known as a “torrent.”

12. A torrent file is a computer file that contains metadata about files and folders to be distributed, and usually also a list of the network locations of trackers, which are computers that help participants in the system find each other and form efficient distribution groups called “swarms.” A torrent file does not contain the content to be distributed; it only contains information about those files, such as their names, sizes, folder structure, and cryptographic hash values (known as “info hashes”) for verifying file integrity. Torrent files are normally named with the extension “.torrent,” as in “MyFile.torrent.”

13. After a Torrent website is queried, the website will provide the user with a list of “.torrent” file(s) that relate to the user’s search.

14. After the user selects and downloads a “.torrent” file that matches his/her search query, the user can download the actual files of interest only through a direct connection to the computer(s) sharing the actual file. This direct connection is accomplished through a P2P BitTorrent software program.

15. For example, a person interested in obtaining child pornographic images would access a Torrent website on his/her Internet browser and conduct a keyword search for files using terms such as “preteen sex.” The Torrent website sends out the search query over the network of computers using compatible P2P software. The results of the search are returned to the user’s computer and displayed on the Torrent website. The user selects the file(s) he/she wants to download from the results displayed on the Torrent website. Once the “.torrent” file is downloaded, it is used by a BitTorrent P2P software program, which the user must have previously installed, to download the child pornography files directly from the computer sharing

the files. The downloaded files are stored in an area on the user's computer that was previously designated by the user and/or the software. The downloaded file will remain on the user's computer until moved or deleted by the user.

16. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a BitTorrent user downloading an image file may actually receive parts of the image from multiple computers. The advantage to this is that it speeds up the time it takes to download the file. Often, however, a user downloading a file receives the entire file from one computer.

17. A P2P file transfer is assisted by reference to an IP address. This address, expressed as four numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location, making it possible for data to be transferred between computers.

18. The computer running the file-sharing application, in this case BitTorrent, has an IP address assigned to it while it is on the Internet. Investigators are able to see the IP address of any computer system sharing files. Investigators can then search public records (e.g., the American Registry of Internet Numbers at www.arin.net) that are available on the Internet to determine the ISP who has assigned that IP address. Based upon the IP address assigned to the computer sharing files, subscriber information can be obtained from the Internet service provider.

VII. STATEMENT OF PROBABLE CAUSE

19. On or about January 12, 2018, I received information from SA Joseph Cecchini, an FBI agent assigned to the FBI office located in Tulsa, Oklahoma, regarding a BitTorrent file-sharing investigation he conducted on or about December 8, 2017. I learned the following from reading SA Cecchini's reports:

a. On or about December 8, 2017, between 5:16 a.m. and 9:29 a.m. Central Time Zone, SA Cecchini used a BitTorrent application to conduct an undercover investigation into the Internet sharing of child pornography. During this investigation, a computer sharing suspected child pornography was located on the BitTorrent file-sharing network. SA Cecchini downloaded over 100 images and videos containing the sexual exploitation of children, including child erotica and child pornography, from a computer using an IP Address of 71.94.139.132 (the "SUSPECT IP ADDRESS"). Many of the downloaded files depict the sexual exploitation of a child that appears to be under thirteen years old.

b. As previously described, BitTorrent identifies a collection of shared files though a unique value, referred to as an info hash. The Torrent info hash in this investigation was "afe6097d6baf3040f3ac32e275aab06b524dab51." This unique info hash identified a BitTorrent collection of approximately 749 files. SA Cecchini downloaded over 100 files in this collection from a computer that was using the SUSPECT IP ADDRESS. In my subsequent review of the downloaded content, I observed what appeared to be files containing child pornography.

c. SA Cecchini used the American Registry for Internet Numbers ("ARIN") and confirmed that the SUSPECT IP ADDRESS was registered to the ISP Charter Communications.

20. On or about July 3, 2018, I again reviewed the files that SA Cecchini downloaded from the SUSPECT IP ADDRESS, and observed videos and images depicting what appear to be child pornography. The following are three examples of the suspected child pornography I observed:

a. “2007 Tara 8Yr - Collection - It hurts Daddy” – this video depicts what appears to be a female under thirteen years old rubbing her own genitals and performing sexual acts with an adult male. Sex acts include intercourse and digital penetration of her anus by a foreign object.

b. “tara 5yr 017.jpg” – this image depicts what appears to be a nude female under thirteen years old sitting on top of a nude adult male. The adult male penetrates the minor female’s genitals with his penis.

c. “2007 Tara 8yr - watches porn and masturbates - July 12, 2007” – this video depicts what appears to be a female under thirteen years old. The minor is naked sitting on a chair. She is masturbating while watching adult pornography on a computer monitor.

VIII. IDENTIFICATION OF SUBSCRIBER OF SUSPECT IP ADDRESS

21. I have reviewed the subscriber account information from Charter Communications for the SUSPECT IP ADDRESS. According to Charter Communications, for the time period of November 18, 2017, to April 20, 2018, which encompasses the times in which the SUSPECT IP ADDRESS was used by a computer to distribute child pornography, the SUSPECT IP ADDRESS was assigned to an account subscribed to “Cristobal Hernandez” at the SUBJECT PREMISES.

22. On or about January 15, 2018, I reviewed Cristobal Hernandez’s California Department of Motor Vehicle (“DMV”) records dated on or about January 11, 2018. According

to DMV records, Hernandez's current address of record is the SUBJECT PREMISES and has lived at the SUBJECT PREMISES since April 21, 2017, which includes the date in December 2017 that SA Cecchini downloaded suspected child pornography from the SUSPECT IP ADDRESS assigned to the SUBJECT PREMISES.

23. On or about May 22, 2018, an FBI air site survey was conducted at the SUBJECT PREMISES. An air site survey was requested because the SUBJECT PREMISES is located behind another residence adjacent to the street. The majority of the SUBJECT PREMISES cannot be viewed from the street, and a drive way that leads to the SUBJECT PREMISES was gated.

24. The FBI air site survey identified a vehicle, a 2011 Honda with California license plate 6SDL669, on the driveway adjacent to the SUBJECT PREMISES. On or about May 24, 2018, I learned from a DMV database that this vehicle was registered to Jimenez Celso Hernandez. Jimenez Celso Hernandez's address was listed as 1535 Elm Avenue, Long Beach.

25. On or about May 31, 2018, I reviewed a United States Postal Service's Change of Address form for Cristobal Hernandez dated May 31, 2018. According to the form, Hernandez started service at the SUBJECT PREMISES on or about March 28, 2017.

26. On or about July 3, 2018, I reviewed a National Comprehensive Report ("NCR") records check for Cristobal Hernandez. NCR is a report generated by Thomson Reuters, which is a company that consolidates public records, including addresses, driver licenses, property deed transfers, and corporate information, as well as some propriety records. According to NCR, Hernandez's most recent address was listed as the SUBJECT PREMISES.

27. Based on the information above, there is probable cause to believe that someone at the SUBJECT PREMISES possessed, and made available for distribution, multiple files

containing child pornography on or about December 8, 2017, that the same individual continues to reside at the SUBJECT PREMISES, and that a search of the SUBJECT PREMISES will yield evidence of the violations stated above.

**IX. TRAINING AND EXPERIENCE ON INDIVIDUALS
WITH A SEXUAL INTEREST IN CHILDREN**

28. As set forth above, someone at the SUBJECT PREMISES appears to possess dozens of child pornography files, and is making these files available to others. Based on the facts set forth above, it is my opinion that there is probable cause to believe that someone at the SUBJECT PREMISES is sexually interested in children and collecting images of the sexual exploitation of children. Based on my training and experience, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who view and possess multiple images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or in other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

c. The child pornography distributed from the SUBJECT PREMISES was in digital format and stored on a digital device. Digital child pornography on a digital device is easy to maintain for long periods of time. Modern digital devices often have extremely large storage capacities. Furthermore, cheap and readily available storage devices, such as thumb drives, external hard drives, and compact disks make it simple for individuals with a sexual interest in children to download child pornography from the Internet and save it – simply and securely – so it can be accessed or viewed indefinitely.

29. Furthermore, even if the individual at the SUBJECT PREMISES deleted any images of child pornography that he/she may have possessed or distributed, there is still probable cause to believe that there will be evidence of the illegal activities – that is, the possession and distribution of child pornography – at the SUBJECT PREMISES. Based on my training and experience, as well as my conversations with digital forensic experts, I know that remnants of such files can be recovered months or years after they have been deleted from a computer device. Evidence that child pornography files were downloaded and viewed can also be recovered, even after the files themselves have been deleted, using readily available forensic tools. Because remnants of the possession, distribution, and viewing of child pornography is recoverable after long periods of time, and because there is probable cause to believe that a user at the SUBJECT PREMISES possessed and shared child pornography on or about December 8, 2017, there is probable cause to believe that evidence of that child pornography will be found at the SUBJECT PREMISES.

X. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

30. As used herein, the term “digital device” includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop,

laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled

environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains

a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime,

indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

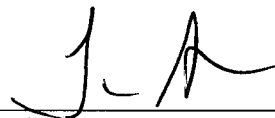
g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is

necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime. In addition, decryption of devices and data stored thereon is a constantly evolving field, and law enforcement agencies continuously develop or acquire new methods of decryption, even for devices or data that cannot currently be decrypted.

31. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

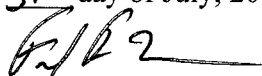
XI. CONCLUSION

32. For all the reasons described above, there is probable cause to believe that the evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) (receipt and distribution of child pornography), and 2252A(a)(5)(B) (possession of child pornography), as described in Attachment B, will be found in a search of the SUBJECT PREMISES.



Timothy Alon, Special Agent
Federal Bureau of Investigation

Subscribed to and sworn before me
This 31st day of July, 2018.

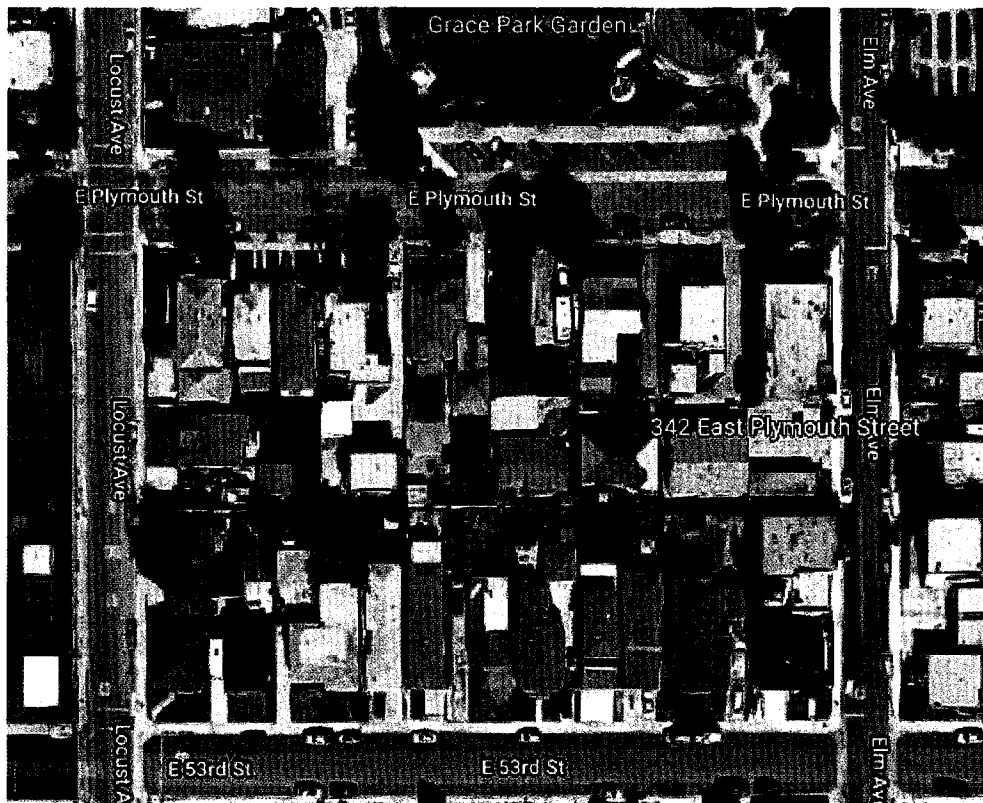


HONORABLE FREDERICK F. MUMM
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PREMISES TO BE SEARCHED

The premises to be searched is the property located at 342 E. Plymouth Street, Long Beach, California 90805 (the "SUBJECT PREMISES"), which is located on a single lot shared with another single-family residence identified as 340 E. Plymouth Street. The 340 E. Plymouth Street residence is the building located adjacent to E. Plymouth Street and has the number "340" at the front of the residence. The SUBJECT PREMISES is located behind the 340 E. Plymouth Street residence. A shared brick styled driveway on the east side of the property leads to the SUBJECT PREMISES at the rear of the property. On the driveway near the sidewalk are two mailboxes. They are labeled "340" and "342."



The SUBJECT PREMISES's exterior walls are dark green in color. A black security door is at the front of the residence. Leading to the front door are two steps. Large windows with white window frames are located on both sides of the front door. Sliding doors are located on the west side of the property. The roof appears to be composed of multi-colored shingles.



ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) (receipt and distribution of child pornography), and 2252A(a)(5)(B) (possession of child pornography) (the “Subject Offenses”), namely:

- a. Child pornography, as defined in 18 U.S.C. § 2256(8).
- b. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that refer to child pornography, as defined in 18 U.S.C. § 2256(8), including but not limited to documents that refer to the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography.
- c. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, tending to identify persons involved in the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography, as defined in 18 U.S.C. § 2256.
- d. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that refer or relate to any production, receipt, shipment, order, request, trade, purchase, or transaction of any kind involving the transmission through interstate commerce by any means, including by computer, of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.
- e. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, identifying persons transmitting in interstate commerce,

including by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

f. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that identify any minor visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

g. Any and all records, documents, programs, applications, or materials or items which are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as “child erotica” and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings.

h. Any records, documents, programs, applications, or materials identifying possible minor victims depicted in child pornography and/or minor victims of sexual abuse.

i. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, which pertain to P2P file sharing software.

j. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, which pertain to accounts with any Internet Service Provider.

k. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, regarding ownership and/or possession of 342

E. Plymouth Street, Long Beach, California 90805 (the “SUBJECT PREMISES”).

l. Records, documents, and material relating to IP address 71.94.139.132 (the "SUSPECT IP ADDRESS").

m. Records, documents, programs, applications, materials, and files relating to the deletion, uploading, and/or acquisition of victim files to include photographs, videos, e-mails, chat logs, or other files.

n. Records, documents, programs, applications, materials, and files relating to the online social media accounts of any victim.

o. Any digital device used to facilitate the above-listed violations and forensic copies thereof.

p. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

q. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized.

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

- iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;
- v. evidence of the times the device was used;
- vi. passwords, encryption keys, and other access devices that may be necessary to access the device;
- vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;
- viii. records of or information about Internet Protocol addresses used by the device;
- ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral

input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the “search team”) will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, “hidden,” or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as “EnCase” and “FTK” (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques, including to search for known images of child pornography.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.